Крезова Татьяна Николаевна

Подписан: Крезова Татьяна Николаевна
DN: OU=ВРИО заведующего, O="МКДОУ "" Детский сад № 19"""", CN=Крезова Татьяна Николаевна, E=dets.sad2013@yandex.ru
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2022.04.13 13:36:16+03'00'
Foxit PDF Reader Версия: 11.2.1

ПРИНЯТО
Общим собранием работников
МКДОУ «Детский сад № 19»
Протокол № 2 от 18.02.2022

УТВЕРЖДАЮ
и. о. заведующего МКДОУ
МКДОУ «Детский сад № 19»
_____Т.Н. Крезова
Приказ № 34/03-05 от 18.02.2022

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном казенном дошкольном образовательном учреждении «Детский сад № 19»

1. Общие положения

Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в муниципальном казенном дошкольном образовательном учреждении «Детский сад № 19» (далее - МКДОУ), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.1. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.2. Для обработки ПДн, необходимых для предоставления государственных и муниципальных услуг МКДОУ, используется информационная система персональных данных (далее - ИСПДн) «АИС «Аверс», предназначенная для осуществления деятельности МКДОУ согласно действующего законодательства.

1.3. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в МКДОУ, в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн «АИС «АВЕРС» и ИСПДн «1С: «Зарплата и кадры».

1.4. Пользователем ИСПДн (далее - Пользователь) является сотрудник МКДОУ, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее - СЗИ) ИСПДн.

1.5. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн МКДОУ, проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в МКДОУ и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценка уровня осведомленности и знаний работников МКДОУ в области обработки и защиты персональных данных
- оценка обоснованности и эффективности применяемых мер и средств защиты.

1. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

1.1. Проверки соответствия обработки ПДн установленным требованиям в МКДОУ разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

1.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План, приложение1) и предназначены для осуществления контроля выполнения требований в области защиты информации в МКДОУ.

1.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн МКДОУ.

1.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

1.4.1. По результатам расследования инцидента информационной безопасности;

1.4.2. по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

1.4.3. по решению заведующего МКДОУ.

2. Планирование контрольных мероприятий

2.1.Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

2.2.План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

2.1.1. цели проведения контрольных мероприятий;

2.1.2. задачи проведения контрольных мероприятий,

2.1.3. объекты контроля (процессы, подразделения, информационные системы и т.п.);

2.1.4. состав участников, привлекаемых для проведения контрольных мероприятий;

2.3. сроки и этапы проведения контрольных мероприятий.

Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

3.Оформление результатов контрольных мероприятий

3.1.По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

3.2.По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

3.2.1. описание проведенных мероприятий по каждому из этапов;

3.2.2. перечень и описание выявленных нарушений;

3.2.3. рекомендации по устранению выявленных нарушений;

3.2.4. заключение по итогам проведения внутреннего контрольного мероприятия.

3.3. отчет передается на рассмотрение руководству МКДОУ.

3.4. Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета событий информационной безопасности.

3.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКДОУ (приложение 2).

4. Порядок проведения плановых, внеплановых контрольных мероприятий

4.2. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных МКДОУ.

4.3. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

4.4. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

— Соответствие полномочий Пользователя правилам доступа.

— Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.

— Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в МКДОУ.

— Соблюдение Порядка доступа в помещения МКДОУ, где ведется обработка персональных данных.

— Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.

— Знание Администраторамиинструкций и регламентов по обеспечению безопасности информации в МКДОУ.

— Порядок и условия применения средств защиты информации.

— Состояние учета машинных носителей персональных данных.

— Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.

— Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

— Технические мероприятия, связанные со штатным и нештатным функционированием средств защиты.

— Технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

Приложение 1
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	**Периодичность регулярных мероприятий**	**Периодичность плановых мероприятий**	**Исполнитель**
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС СПО	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных

Контроль обеспечения резервного копирования		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз		Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	Ответственный за организацию обработки ПДн в
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	

Приложение 2
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

ПРОТОКОЛ №

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКДОУ «Детский сад № 19»

Настоящий Протокол составлен в том, что «_____» _____ 20_г.
_____ (комиссией)
(должность, Ф.И.О. сотрудника)
проведена проверка _____
(тема проверки)
Проверка осуществлялась в соответствии с требованиями:
(название документа)
В ходе проверки проверено:
Выявленные нарушения:
Меры по устранению нарушений:
Срок устранения нарушений:_____
Председатель комиссии:
фамилия и инициалы / подпись / должность
Члены комиссии:
фамилия и инициалы / подпись / должность фамилия и инициалы /подпись / должность

ЛИСТ ОЗНАКОМЛЕНИЯ:

Романенко С.А. _____

Крезова Т.Н._____

Курбатова О.А._____

Меньшикова Н.А._____

Масалова В.В._____

Минько О.В._____

Цыс М.С._____